

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BOARD OF PATENT APPEALS AND INTERFERENCES**

In re patent application of:) Date: May 14, 2008
Frank S. Saavedra-Lim) Attorney Docket No.: E-833
Serial No.: 09/475,950) Customer No.: 00919
Filed: December 13, 1999) Group Art Unit: 3627
Confirmation No.: 7103) Examiner: Mussa A. Shaawat
Title:	METHOD AND SYSTEM OF UPGRADING THIRD PARTY FUNCTIONALITY IN AN ELECTRONIC FRAUD MANAGEMENT SYSTEM

APPELLANT'S BRIEF ON APPEAL

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The appellants respectfully submit the following brief in the appeal of the subject application. The Notice of Appeal was filed on March 25, 2008, following a Final Office Action mailed December 27, 2007.

TABLE OF CONTENTS

- I. REAL PARTY IN INTEREST
- II. RELATED APPEALS AND INTERFERENCES
- III. STATUS OF CLAIMS
- IV. STATUS OF AMENDMENTS
- V. SUMMARY OF CLAIMED SUBJECT MATTER
- VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL
- VII. ARGUMENT
- VIII. CLAIMS APPENDIX
- IX. EVIDENCE APPENDIX
- X. RELATED PROCEEDING APPENDIX

I. Real Party in Interest

Pitney Bowes Inc. is the real party interest.

II. Related Appeals and Interferences

There are no related Appeals and Interferences.

III. Status of Claims

- (a) Claims 1-6 and 9-14 are in the application.
- (b) Claims 7 and 8 have been canceled.
- (c) Claims 1-6 and 9-14 are rejected.
- (d) Claims 1-6 and 9-14 are on appeal.

IV. Status of Amendments

An Amendment subsequent to the Final Rejection of December 27, 2007, was filed on February 26, 2008. This Amendment was not entered.

V. Summary of Claimed Subject Matter

Within the financial industry in general there is a marked propensity for fraud, which thus associates a certain degree of risk with each transaction or financial product introduction. This is particularly true in the credit card portion of the industry. Case history supports this conclusion. Fraud can, and does, originate both internally to the organization issuing the financial product, and externally, with customers, vendors, merchants, or criminals that intercept the communication of credit card information, electronically, or physically. Thus, fraud in this industry is expected.

Fraud is inherent in how credit cards are issued and handled. There is, for example, no significant threat to the issuer of a card from someone finding a lost credit card and using it to purchase gas in an automated gas station; and, telephone and mail orders may be made by criminals illegally possessing credit account information. In the same category, a fraudulent

merchant may be operating fraudulently by selling merchandise on unequal consideration. On a larger scale, however, fraud rings are particularly active and include many players in their networks that defraud issuers of billions of dollars. Rogue employees and questionable merchants account for a significant part of skimming activity, which involves the illegal acquisition of account information in order to produce counterfeit cards or make fraudulent transactions. The sophistication of skimming is quite advanced in that criminals may wait up to eighteen to twenty (18-20) months after skimming a card before they use it. This category of fraud which originates at the point of sale is expected to be a twenty five billion dollar (\$25,000,000,000) problem in 1999.

Recent security conference statistics show that distinct trends emerge from studies of fraud. The top fraud types are lost, stolen, or counterfeit credit cards or accounts. Fraud losses resulting from lost and stolen credit cards (plastic) represent nearly sixty percent (60%) of all losses, with the fourth (4th) quarter of any year being the top fraud period. The hours of 12:00 Noon to 10:00 PM are the peak fraud activity times; California, Florida and New York are the top fraud states; and, Los Angeles, New York City, and Las Vegas are the top fraud cities. Telemarketing, phone use, and gas purchases are the top fraud industry groups.

While it is evident that fraud exists, and that it is extremely difficult to eliminate, even in the current technological environment, actions can be taken to control the impact of fraud. The credit card industry is not totally defenseless when it comes to fraud. It is evident that acquirers (merchants), issuers (banks), the major credit card associations (ie., VISA® and MasterCard®), and third party vendors are making their best efforts to stay on top of the issue. The theme of fraud management is currently one promoting early detection and warning and loss mitigation as close as possible to the point of sale. There are a number of industry tools that are being employed to manage fraud and risk accordingly.

Applications for credit cards undergo scrutiny from such industry watchdogs and utilities as the VISA ICS (Issuer's Clearinghouse Service), from general information validation procedures, and from credit bureau fraud screen products such as SAFESCAN from Equifax, HAWK from TransUnion, or FACS from Experian. Transaction processing too, undergoes scrutiny from such industry methods as: the Fair Isaac Consumer Score (FICO); the Falcon - Neural Network Model (HNC); NESTOR - Neural Network Model; Queue Based Fraud Detection (TSYS DFS); the VISA Consumer Risk Score (CRIS); and, the VISA Magnetic Code Verification (CVV/CVC).

While the industry has taken steps to safeguard against fraud, it is recognized that the

existing fraud detection technology (such as making calls to cardholders when a fraud is suspected) can impact desired customer service and convenience. Therefore, a balance is required in the state of fraud management that will allow the industry to protect itself while remaining commercially viable.

One aspect of progressive fraud management is the development of a concept, structure and effective method for allowing fraud to be identified, measured, and proactively managed at the task level. Another requirement for effective fraud management is the development of an ability to benchmark against the industry.

Appellants claimed invention claims a method that assesses a set of risks relative to granting credit on a financial product by applying a fraud to each assessment wherein the fraud is selected from a list of fraud that is representative of a defined area of risk.

Claim 1 is the only independent claim in this Patent Application.

Claim 1 relates to a method of managing and assessing a set of risks relative to a financial product, said method being accessed through a data processing system, wherein said data processing system comprises a series of nodes operatively connected with each other, the method includes the following steps: (a) performing an application processing procedure on one or more customers, comprising a check of the creditworthiness of one or more selected customers; and issuing a financial product to one or more of said customers if said selected customer is determined to be creditworthy, thus resulting in an accepted customer, and declining said application if said customer is determined to be not creditworthy; (Fig. 10, step 900)

(b) assessing a credit authorization request from a system user, wherein said request is initiated by a use of said financial product; (Fig. 10, step 901)

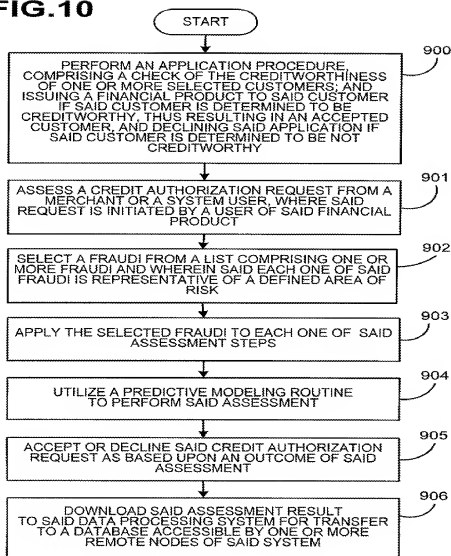
(c) utilizing a predictive modeling routine to perform said assessment; (Fig. 10, step 904)

(d) accepting or declining said credit authorization request as based upon an outcome of said assessment; (Fig. 10, step 905)

(e) downloading an assessment result to said data processing system for transfer to a database accessible by one or more remote nodes of said system; (Fig. 10, step 906)
and

(f) applying a fraud indicator to each assessment and wherein said fraud indicator is selected from a list of fraud indicator and wherein each of said fraud indicator on the list is representative of a defined area of risk. (Fig. 10, step 903).

FIG.10



According to the invention, the object is achieved and the disadvantages of the prior art are overcome by a method for managing and assessing a set of risks relative to a financial product, wherein the method is accessed through a data processing system. The data processing system comprises a series of nodes operatively connected with each other. The method begins by performing an application processing procedure, comprising a check of the creditworthiness of one or more selected customers; and issuing a financial product to the selected customer if that customer is determined to be creditworthy; and, declining the application if the customer is determined to be not creditworthy.

After the card has been issued to a customer, the use of the card is assessed whenever the card is presented for payment of goods or services or to obtain a cash advance. The

assessment is made as the result of a credit authorization request from a merchant or a system user and utilizes a predictive modeling routine to perform the assessment. The credit authorization is accepted or rejected based upon an outcome of the assessment. The assessment results are then downloaded to the data processing system for transfer to a database accessible by one or more remote nodes of the system.

The assessment itself further comprises the steps of applying a transaction procedure to determine whether or not the credit authorization request is to be accepted or declined, and then applying a fraud set (fraud indicator) to the assessment methodology. The fraud set serves to identify a set of risks associated with each step of the assessment. The credit authorization assessment methodology further comprises the steps of: performing a set of pre-processing checks; performing a set of transaction approval checks; performing a set of post processing checks; and, making a set of post approval account adjustments required as a result of a credit authorization approval. On an individual transaction basis, each transaction can be accepted or declined based upon an outcome of the assessment.

Any of the transactions, assessments, or determinative calculations can be retained as a means of continually refreshing the pool of data available for credit determinations.

Claim 1 is the only independent claim in this patent application that is on appeal. Claim 1 is a method of managing and assessing a set of risks relative to a financial product. The method being accessed through a data processing system, wherein the data processing system comprises a series of nodes operatively connected with each other. Appellant's invention which is shown in Fig. 10 (a copy of which appears next to this page) and was added to page 28, of the specification by a September 17, 2002 entered Amendment which reads as follows:

"After the program starts, the program goes to block 900. In block 900, the program performs an application procedure, comprising a check of the creditworthiness of one or more selected customers; and issuing a financial product to said customer if said customer is determined to be creditworthy, resulting in an accepted customer, and declining said application if said customer is determined to be not creditworthy. Then the program goes to block 901 to assess a credit authorization request from a merchant or a system user, where said request is initiated by a user of said financial product. Now the program goes to block 902 to select a fraud from a list comprising one or more fraud and wherein said each one of said fraud is representative of a defined area of risk. Then the program goes to block 903 to apply the selected fraud to each one of said assessment steps. Then the program goes to block 904 to utilize a predictive modeling routine to perform said assessment. Now the program goes to block 905 to accept or decline said credit authorization request as based upon an outcome of said assessment. Then the program goes to block 906 to download said assessment result to said

data processing system for transfer to a database accessible by one or more remote nodes of said system."

VI. Grounds of Rejection to be Reviewed on Appeal

Whether or not claims 1-6, and 9 - 14 are patentable under 35 use § 103 (a) over Lebda et al. (U.S. Patent 6,385,594) in view of Keen et al. (U.S. Patent 5,774,882).

VII. Argument

Claims 1-6, and 9 - 14 have been rejected by the Examiner under 35 USC § 103 (a) over Lebda et al. (U.S. Patent 6,385,594) in view of Keen et al, (U.S. Patent 5,774,882).

A. Claims 1 - 3, 5 - 6 and 9 -10

Lebda discloses the following in line 58 of col. 1 - line 17 of col. 2:

"To achieve these and other objects of the invention, there is provided a method and apparatus for coordinating an electronic credit application between an Internet user and a plurality of lending institutions via the Internet. The method comprises the steps of displaying a plurality of documents to an Internet user, receiving a plurality of credit data sent from the Internet user; matching an electronic credit application to a filter comprising a plurality of selection criteria; transmitting the credit data to a plurality of lending institutions via one of four methods; and responding to the Internet user via the Internet. The documents sent to the Internet user includes a series of questions pertaining to their desired loan, followed by the appropriate type of loan application. The various types of loan applications include first and second mortgages, car loans, student loans, personal loans, and credit card applications.

Other types of credit applications may exist without departing from the spirit of the invention. Upon completion of the application, the invention matches a unique filter to the credit data entered by the Internet user.

The filter is made up of a plurality of selection criteria in which a specific lending institution has given to the inventor. The filter is customizable by the specific lending institution in real time and unique to each lending institution. Once the application has been filtered, it is sent to a list of lending institutions that match with the credit application. These lending institutions then reply as to whether the application has been accepted or rejected."

Lebda performs a credit check on someone when they apply for a loan or financial product.

Keen discloses the following in line 48 of col. 3 to line 17 of col. 4.

"If the credit application is a corporate application, the application information is sent to the corporate queue 90 for processing. The fact that the application 45 is a corporate application is sent to tallies 190 to be tabulated and recorded. Preferably a database program can tabulate and store this data on the system memory for future applications and audits. Preferably, the final decision whether to grant a corporate application would be the Corporate Manager's responsibility, therefore it is not processed in the same manner as individual applications. However, the application information is stored in the system, and a credit report from a nationwide credit bureau 130 may be accessed and matched with the application information. Each credit report is kept on line and active until a final decision is made. This serves to speed the decision making process for corporate applications by correlating important credit history information and making that information easily available to those terminals connected to the system.

If the application is from an individual, discrepancies between the post mark and the mailing address 100 are checked by the main system processor 10. The application's post marked envelope is scanned by scanner 40 and OCR unit 42. The envelope contains only one AOI region of interest. That area is the postmark area in the upper right corner of the envelope. The scanned and OCR-converted postmark is compared to the mailing address. A discrepancy would be found if the postmark was from California, but the applicant's mailing address was listed as being New York. If there is such a discrepancy between the post mark and the mailing address, the system processor 10 will prompt the mail room to write the postmark's origin or otherwise put the postmark on the application 110. The main processor preferably sends the digitally scanned images of both the scanned application and the post mark to security terminal 20 to verify the existence of any attempt at fraud in the application. Verified fraud 120 would be established after locating and talking with the suspected victim."

Keen performs a credit check on an application for credit.

Neither Lebda or Keen taken separately or together disclose or anticipate steps b-f of claim 1, namely (b) assessing a credit authorization request from a system user, wherein said request is initiated by a use of said financial product;

(c) utilizing a predictive modeling routine to perform said assessment; ;(d) accepting or declining said credit authorization request as based upon an outcome of said assessment; (e) downloading an assessment result to said data processing system for transfer to a database accessible by one or more remote nodes of said system; and (f) applying a fraud indicator to each assessment and wherein said fraud indicator is selected from a list of fraud indicator and wherein each of said fraud indicator on the list is representative of a defined area of risk.

Notwithstanding the foregoing, in rejecting a claim under 35 U.S.C. §103, the Examiner

is charged with the initial burden for providing a factual basis to support the obviousness conclusion. *In re Warner*, 379 F.2d 1011, 154 USPQ 173 (CCPA 1967); *in re Lunsford*, 375 F.2d 385, 148 USPQ 721 (CCPA 1966); *in re Freed*, 425 F.2d 785, 165 USPQ 570 (CCPA 1970). The Examiner is also required to explain how and why one having ordinary skill in the art would have been led to modify an applied reference and/or combine applied references to arrive at the claimed invention. *In re Ochiai*, 37 USPQ2d 1127 (Fed. Cir. 1995); *in re Deuel*, 51 F.3d 1552, 34 USPQ 1210 (Fed. Cir. 1995); *in re Fritch*, 972 F.2d 1260, 23 USPQ 1780 (Fed. Cir. 1992); *Uniroyal, Inc. v. Rudkin-Wiley Corp.*, 837 F.2d 1044, 5 USPQ2d 1434 (Fed. Cir. 1988). In establishing the requisite motivation, it has been consistently held that both the suggestion and reasonable expectation of success must stem from the prior art itself, as a whole. *In re Ochiai*, supra; *in re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991); *in re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988); *in re Dow Chemical Co.*, 837 F.2d 469, 5 USPQ2d 1529 (Fed. Cir. 1988).

B. Claim 4

Claim 4 depends on claim 1. In claim 4 the accepted customer is an individual and wherein an account is representative of a business affiliation and said set of risks is a function of an individual's profile.

In addition to the arguments made in above Section A please consider the following.

The cited art is not concerned with accessing the risk of a financial product when the request is initiated by the use of the financial product as claimed in claim 4. In claim 4, Appellant's set of risks is a function of an individual's profile. In addition to the comments made in above paragraph A, the cited art does not disclose a set of risks that are a function of an individual's profile.

C. Claims 11-14

In addition to the arguments made in above Section A please consider the following.

The Examiner indicated the following in page 5 of the Final Rejection.

"Regarding claims 11-14, Lebda et al. do not explicitly disclose benchmarking risk management effectiveness by determining fraud loss ratios, including the ratio of fraud loss to any of portfolio maturity, volume of total sales, or total charge-offs. However, benchmarking risk management effectiveness by determining fraud loss ratios, including the ratio of fraud loss to any of portfolio maturity, volume of total sales, or total charge-offs, is certainly well known to those of ordinary skill in the art, and official notice to that effect is hereby taken. Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention, to have modified the method of Lebda et al., so as to include benchmarking risk management effectiveness by determining fraud loss

ratios, including the ratio of fraud loss to any of portfolio maturity, volume of total sales, or total charge-offs, as is well known to do, in order to track and understand the effectiveness of the risk management program, since so doing could be performed readily and easily by any person of ordinary skill in the art, with neither undue experimentation, nor risk of unexpected results."

The specific benchmarking risk of determining fraud loss ratio to benchmark risk management effectiveness (claim 11), measuring fraud losses as a function of portfolio maturity (Claim 12); measuring fraud losses as a function of volume total sales (claims 13) and determining a contribution of fraud losses in total charge offs (claims 14) have not been disclosed or anticipated by the cited art.

Appellant respectfully submits that the final rejection of claims 1 - 6 and 9 -14 is in error for at least the reasons given above and therefore should be reversed.

In conclusion, Appellant respectfully submits that the final rejection of claims 1-6 and 9-14 is in error for at least the reasons given above and should, therefore, be reversed.

Respectfully submitted,

/Ronald Reichman/
Ronald Reichman
Reg. No. 26,796
Attorney of Record
Telephone (203) 924-3854

PITNEY BOWES INC.
Intellectual Property and
Technology Law Department
35 Waterview Drive
P.O. Box 3000
Shelton, CT 06484-8000

VIII. CLAIMS APPENDIX

1. A method of managing and assessing a set of risks relative to a financial product, said method being accessed through a data processing system, wherein said data processing system comprises a series of nodes operatively connected with each other, said method comprising the steps of:

(a) performing an application processing procedure on one or more customers, comprising a check of the creditworthiness of one or more selected customers; and issuing a financial product to one or more of said customers if said selected customer is determined to be creditworthy, thus resulting in an accepted customer, and declining said application if said customer is determined to be not creditworthy;

(b) assessing a credit authorization request from a system user, wherein said request is initiated by a use of said financial product;

(c) utilizing a predictive modeling routine to perform said assessment;

(d) accepting or declining said credit authorization request as based upon an outcome of said assessment;

(e) downloading an assessment result to said data processing system for transfer to a database accessible by one or more remote nodes of said system; and

(f) applying a fraud indicator to each assessment and wherein said fraud indicator is selected from a list of fraud indicator and wherein each of said fraud indicator on the list is representative of a defined area of risk.

2. The method of claim 1, wherein said financial product is a credit card.

3. The method of claim 1, wherein said accepted customer is a business entity.

4. The method of claim 1, wherein said accepted customer is an individual and wherein an account is representative of a business affiliation and said set of risks is a function of an individual's profile.

5. The method of claim 1, wherein said accepted customer is an individual and wherein an account is representative of a business affiliation and said set of risks is a function of a business' profile.

6. The method of claim 1, wherein said accepted customer is an individual, and wherein an account is representative of an individual's and a business' affiliation, and said set of risks is a function of an individual's profile and a business' profile.
9. The method of claim 1, wherein a set of data relative to said credit authorization request is retained in a memory of said data processing system and utilized to determine the effectiveness of an assessment methodology.
10. The method of claim 1, wherein a filtering step comprises a credit score filter for eliminating a portion of a population that does not pass through said filter.
11. The method claimed in claim 1, further including the step of:
determining fraud loss ratios to benchmark risk management effectiveness.
12. The method claimed in claim 11, further including the steps of:
measuring fraud losses function of a portfolio maturity.
13. The method claimed in claim 11, further including the step of;
measuring fraud losses as a function of volume of total sales.
14. The method claimed in claim 11, further including the step of:
determining a contribution of fraud losses in total charge offs.

IX. EVIDENCE APPENDIX

There is no additional evidence to submit.

X. RELATED PROCEEDING APPENDIX

There are no related appeals and interferences.